2019 PRIVACY (GDPR, CCPA, GLBA) SURVEY

EXECUTIVE SUMMARY

DATA COLLECTED: FEBRUARY-MARCH 2019
REPORT DATE: MAY 2019

JOIN. ENGAGE. LEAD.

Operational Risk

ACKNOWLEDGMENTS

This survey was designed in preparation of the RMA Privacy Round Table scheduled for April 8, 2019 in Boston. The Steering Committee members from Bank of the West, BB&T Bank, Capital One Bank, and Fifth Third Bank helped RMA draft questions for this survey.

The purpose of the survey was to capture the current status on privacy issues, such as GDPR, CCPA, and GLBA across a range of RMA member institutions.

The final report provides participants' responses, while protecting the confidentiality of individual institutions by masking the source of the responses.

Note: Due to rounding, percentages in the tables may not add up to 100.

RMA staff contributing to the study included Edward J. DeMarco Jr. and Sylwia M. Czajkowska.

Institutions (33) that participated in the survey:

Anonymous (5)
Amarillo National Bank
Arvest Bank
Associated Bank
Bank of Hawaii
Bank of the West
BankIowa
Branch Banking & Trust Co. (BB&T)
Capital One
Discover Financial Services
Federal Home Loan Bank Pittsburgh
Fifth Third Bank
First Midwest Bank
First Savings Bank
Fulton Bank
Horicon Bank
Huntington Bank
KeyBank
Land Bank of Taiwan
M&T Bank
Morgan Stanley Private Bank NA
MUFG Union Bank
Mutual of Omaha Bank
People's United Bank
PNC Bank

Rabobank
Regions Bank
State Bank of Cross Plains
Umpqua Bank

RMA would like to thank the community banks that participated in this study. Credit for participation was given to all 33 institutions regardless if respondents skipped certain questions or not, yet provided valuable data to the majority of the questions.

Disclaimer

The information contained herein is obtained from sources believed to be accurate and reliable. All representations contained herein are believed by RMA to be as accurate as the data and methodologies will allow. However, because of the possibilities of human and mechanical error, as well as unforeseen factors beyond RMA's control, the information herein is provided "as is" without warranty of any kind, and RMA makes no representations or warranties expressed or implied to a subscriber or any other person or entity as to the accuracy, timeliness, completeness, merchantability, or fitness for any particular purpose of any of the information contained herein. Furthermore, RMA disclaims any responsibility to update the information. Moreover, information is supplied without warranty on the understanding that any person who acts upon it or otherwise changes position in reliance thereon does so entirely at such person's own risk.

The report is provided to participating institutions for internal analytical and planning purposes only. As such, a participating institution may disclose the information to consultants and agents that are engaged to assist that participating institution in analysis and planning; however, such consultant or agent is prohibited from using the information for any purpose other than such analysis and planning for that participating institution.

About RMA

The Risk Management Association (RMA) is a not-for-profit, member-driven professional association serving the financial services industry. Its sole purpose is to advance the use of sound risk management principles in the financial services industry. RMA promotes an enterprise approach to risk management that focuses on credit risk, market risk, operational risk, securities lending, and regulatory issues. Founded in 1914, RMA was originally called the Robert Morris Associates, named after American patriot Robert Morris, a signer of the Declaration of Independence. Morris, the principal financier of the Revolutionary War, helped establish our country's banking system.

Today, RMA has approximately 2,500 institutional members. These include banks of all sizes as well as nonbank financial institutions. RMA is proud of the leadership role its member institutions take in the financial services industry. Relationship managers, credit officers, risk managers, and other financial services professionals in these organizations with responsibilities related to the risk management function represent these institutions within RMA. Known as RMA Associates, more than 18,000 of these individuals are located throughout North America and financial centers in Europe, Australia, and Asia.

Members actively participate in the RMA network of chapters. These chapters are run by RMA Associates on a volunteer basis and they provide our members with opportunities in their local communities for education, training, and networking throughout all stages of their financial services career. Chapters are located across the U.S. and Canada as well as in global financial centers.

RMA members also avail themselves of benefits offered through headquarters in Philadelphia, Pennsylvania. To assist members in advancing sound risk management principles, RMA keeps members informed and provides access to industry information at this site; publishes *The RMA Journal* and a variety of newsletters, books, and statistics; conducts workshops and seminars; holds conferences, including an annual convention (Annual Risk Management Conference); and has numerous committees working on a variety of projects.

Visit RMA at www.rmahq.org.
Note: As a not-for-profit, professional association, RMA does not lobby on behalf of the industry.

EXECUTIVE SUMMARY

In recent years, there has been a large number of new laws and regulations in the data privacy space. Many institutions need to take into consideration multiple changing laws, e.g. General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Gramm-Leach-Bliley Act (GLBA) and translate those data privacy requirements to day-to-day practices. Each of the regulations focuses on protecting sensitive consumer data, which prompts financial institutions to ensure proper governance and manage customers' demands and expectations, while also continuing to grow their position in the market.

The survey was conducted by The Risk Management Association (RMA) between February and March 2019. Most of the questions were multiple choice with opportunities to provide comments. Some questions were open text and designed to provide information and insight about the current state of practices.

A total of 33 responses were received from a wide range of financial institutions including community, regional, and large banks headquartered in the United States.

- Asset size below $10 billion: 7 responses.
- Asset size between $10-50 billion: 12 responses.
- Asset size between $50-100 billion: 4 responses.
- Asset size over $100 billion: 10 responses.

Due to the number of low responses in each of the asset size categories and to prevent discoverability issues, this report will present the overall results.

Approximately 81% of respondents confirmed that their institution is actively working to comply with the California Consumer Privacy Act (CCPA).

When asked if institutions leverage external support to comply with recent privacy regulations, 72% answered "no". Out of those who confirmed using external support, the majority of responses work with external legal counsel. Some institutions also work closely with one of the "big four" accounting firms.

One of the key elements of the CCPA is the data component. In order to ensure that the data is protected and managed properly, there needs to be a person in charge whose responsibility is to oversee the data privacy aspect. When asked who in their institutions oversees data privacy, almost 40% selected the compliance department. About 33% indicated that it is the joint effort of multiple functions, e.g. operational risk management, enterprise data operations, compliance, the chief information security officer, and information risk management.

There was almost an even split in responses when asked if there is a first line business owner for the company's privacy practices.

According to the survey, 78% of the institutions have all privacy regulations (CCPA, GLBA, and GDPR) supported by a centralized department.

Of those surveyed, 54% indicated that the number of full time associates assigned to support the privacy regulations falls in the range between 2 and 5. For 24% of the surveyed institutions the number of full time associates is in the range between 6 and 10. In order to support the upcoming privacy regulations, we asked if in the near future institutions plan on hiring additional full time associates. Approximately 58% of the respondents have no plans to hire additional associates. About 18% predict that they may consider hiring anywhere from 2 to 5 associates.

Almost 68% of responding institutions opted-out of full compliance with GDPR. In a majority of cases, those who opted out did not exit any relationship in order to comply with GDPR.

The next section of the survey focused on emerging domestic laws (such as Arizona, Alabama, South Carolina federal laws), and on the privacy regulations outside of the United States (e.g. India, Brazil, and Canada). In both instances, respondents provided examples on how best to monitor and evaluate the requirements.

When looking at the relationships that institutions have with third-parties, about 69% do not expect that the upcoming privacy regulations will impact the number of third party providers they do business with. None of the respondents believe that these regulations will increase the number of third-parties. However, 31% predict that the number of third-party relationships may decrease.

Insights

Please see the following pages for detailed responses and examples of the range of practices that banks employ in meeting privacy (GDPR, CCPA, and GLBA) expectations.

Thank you to the RMA member banks for contributing to this benchmarking study. The full report is available to those institutions that contributed to the study.